Internetwork Management

Issues in Distributed Network Environments

Network General Corporation delivers intelligent and integrated network analysis solutions that lead the industry. These systems and applications help organizations optimize the performance of heterogeneous LANs, internetworks, and enterprise network environments. Since 1986, the company has engineered the industry's award-winning Protocol Interpretation, standards-based RMON, and artificial intelligence Expert Analysis applications.

Delivering important milestones in true multivendor interoperability and cooperation, Network General's Sniffer technology is the de facto industry standard. The Company maintains qualified sales, service, and support organizations to help customers proactively plan their networks, optimize performance, and achieve maximum network availability. With installations in 90% of Fortune 100 companies and over 3,500 customers worldwide, Network General is the network analysis market share leader.

For more information about Network General's comprehensive products and services, please call 1-800-SNIFFER (1-800-764-3337).

What is Internetworking?

Internetworking encompasses the increasingly complex process of delivering data from one LAN segment to another. In distributed network environments, data traveling across internetwork links can traverse one or more Wide Area Network (WAN) connections. The types of data which travel over internetwork links is rapidly expanding to include client/server applications, fax, video, and voice. Depending on budget and bandwidth requirements, internetwork equipment ranges from inexpensive dial-up modems, to bridges or routers with WAN interfaces, to sophisticated ATM switches.

Given the various types of data traversing the growing range of internetwork links, the task of internetwork management can appear overwhelmingly complex. Traffic must move efficiently between nodes, between LANs, and between LANs and WANs. To effectively manage internetworks, you need to see the packets traveling through internetwork links across multiple segments.

This paper explores the following internetwork management issues:

- Internetwork interface configurations
- Bandwidth management
- Protocol management
- Bridge and router management
- Error management
- Configuration management

Internetworking Interface Configurations

An internetwork interface model represents a method for linking two or more LAN segments to enable a smooth data communications flow. Currently, internetworks utilize one of four distinct interface models:

- Multiple LAN segments connected by bridges or routers
- Point-to-point, leased line wide area connection between two remote routers
- Wide Area Network connection using WAN protocols such as HDLC, X.25, and frame relay between two remote routers
- Multiple LAN segments connected by a high-speed backbone

Each model defines one possible network interface through which data must pass during its transmission across the network. The implementation of an enterprise network may include any or all of these models. While internetwork links help distribute communications and computing capabilities, using a mix of internetwork interface models can make distributed networks more difficult to manage.

The first internetwork interface consists of multiple LAN segments connected by bridges or routers. A variety of LAN topologies (including Ethernet and token ring) can be internetworked using bridges and routers. The bridge or router serves as a segmenting point for network traffic, so that if the network is designed correctly with respect to traffic load, bandwidth on either side of the bridge or router will be adequate for fast, efficient network operation.

When routers connect LANs together, the router interprets the address of each packet at the network layer, if, in fact, each packet has a network address associated with it. Additionally, if the bridge or router is placed between an Ethernet and token ring segment, address translation occurs at the data link layer. Typically there is no need to encapsulate packets for movement across this LAN-to-LAN internetwork interface. In this model, the native frame structure that contains the data on the LAN is already optimized for transport within the LAN, and from LAN to LAN.

For example, in a LAN-to-LAN internetwork interface, the MAC address is used on both sides of the bridge or router, eliminating the need for an additional address scheme. Frame size is optimized for use on the LAN to operate within either the CSMA/CD Ethernet (802.3) environment, or the deterministic Token Ring (802.5) environment. Last, in the LAN-to-LAN model, the transmission times from one device to another on a LAN are short enough, and the transmission media reliable enough that there is no need for additional error checking at the data link layer beyond what the native protocol provides.

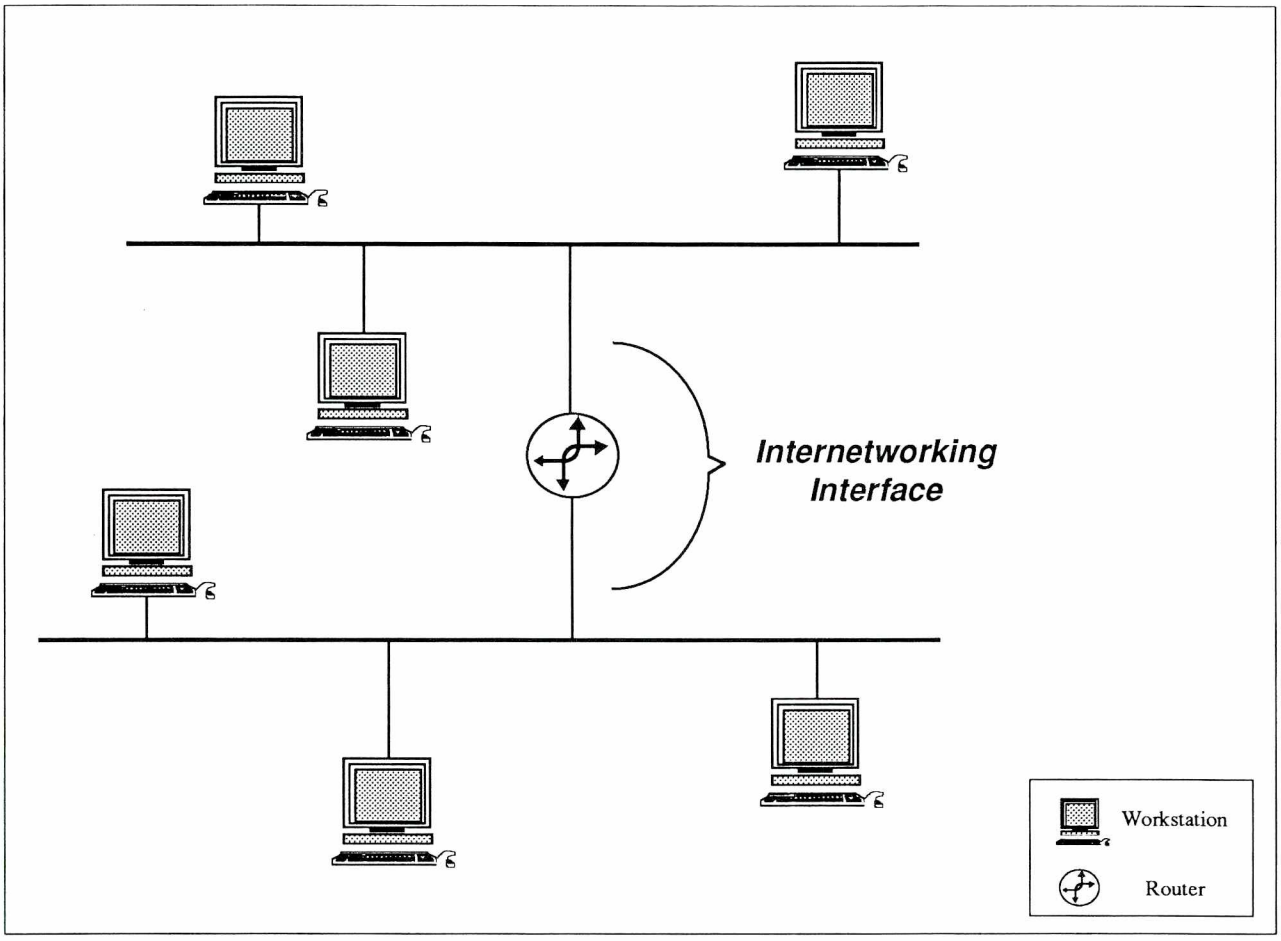

Figure 1: Diagram of LAN-to-LAN internetwork interface

The second model incorporates a point-to-point wide area connection from one router interface to another. For example, two routers are separated by a circuit provided by a telecommunications carrier. The routers repackage the frames received from their respective local area connections in a protocol 'envelope' appropriate to a wide area connection. To reduce expensive leased-line costs, LAN data frames are usually encapsulated within WAN protocols. This requires buffering at the router to minimize bandwidth requirements. Historically, these wide area links have averaged 9600 Kbps, although typical speeds are now 56K, T1 (1.544 Mbps), and even T3 (45 Mbps). This increase in bandwidth allows more traffic from a local LAN to be transferred over the wide area link to a remote LAN more quickly.

Bridge or router proprietary and HDLC-type protocols are popular choices for data encapsulation for several reasons: First, with proprietary protocols, routers or bridges from one vendor can more quickly communicate with another router or bridge from the same vendor, due to the unique header information that each device appends to the transmitted frame. Second, with HDLC, built-in error checking is available on the wide area link at the data link layer. This error checking may not always be available in the native Ethernet or token ring frame format. When network addresses are not available within a given protocol (e.g. NetBIOS, DEC LAT), LAN data is bridged, rather than routed, from the LAN onto the wide area link.

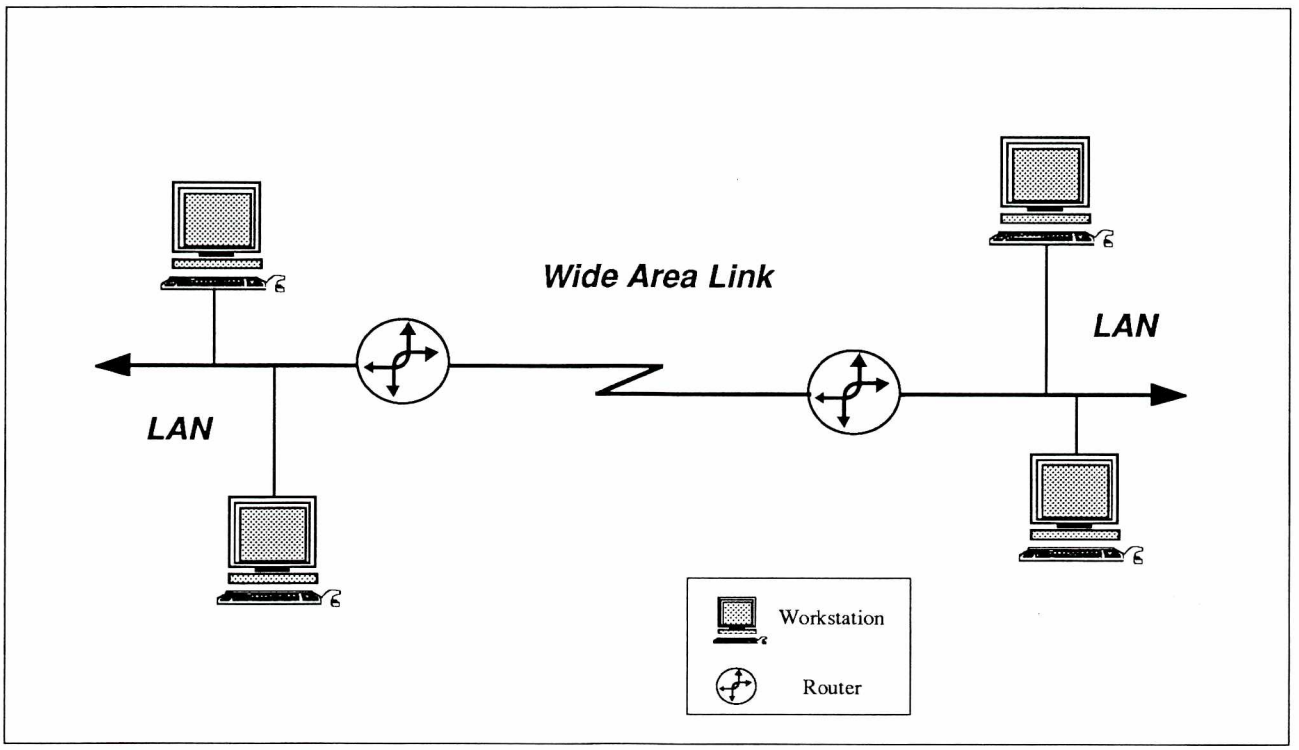

Figure 2: Diagram of WAN link network interface

The third model substitutes a Wide Area Network (WAN) for the wide area link. In this scenario, the packets passing onto the WAN are encapsulated by the bridge or router using common WAN protocols such as HDLC, X.25, and frame relay. The WAN operates between two remote bridges or routers. WAN data rates for internetworking (vs. terminal access) range from 56K to T1. Frames transmitted from a local router must conform to the same protocol being used by the public WAN provider in order to transfer the frames to a remote router.

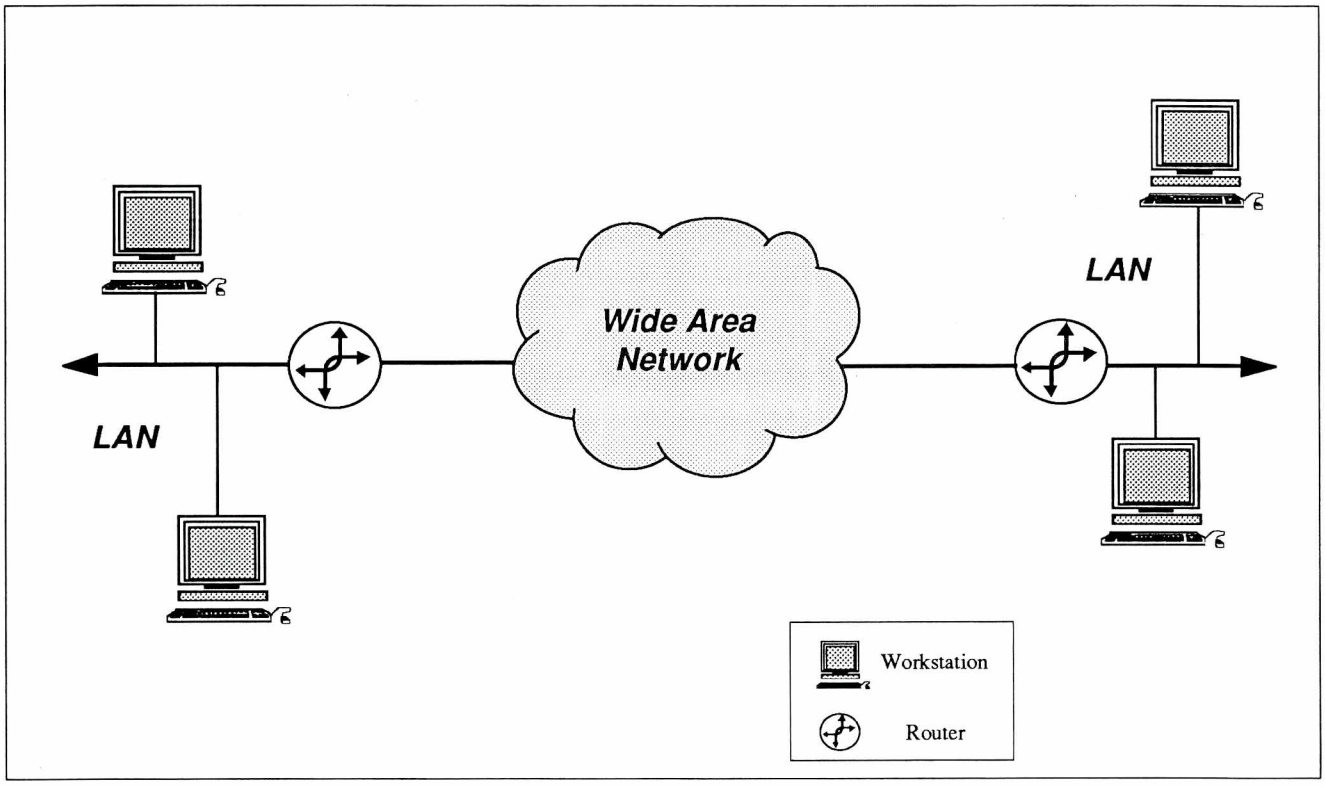

Figure 3: Diagram of WAN network interface

The fourth model continues to evolve as high-speed media access technologies become viable. In this scenario, multiple LAN segments connect to a high-speed backbone to better facilitate the transfer of data between each of the segments. At this time, high-speed backbone technologies include Fiber Distributed Data Interface (FDDI), switched Ethernet using data rates in the Gbps range, and Asynchronous Transfer Mode (ATM). To monitor and manage these high-speed connections and protocols, the management device must be capable of capturing traffic from the backbone segment at the current speed. Purchasing sufficient bandwidth and standards-based technology help lay the groundwork for implementing and managing high-speed media access technologies in the future.

As organizations take advantage of these internetwork models to further expand distributed networks, the challenge of managing the enterprise takes on mission-critical importance. Efficient flow of data across distributed networks necessitates effective management of internetwork links, both from the device and the segment perspective.

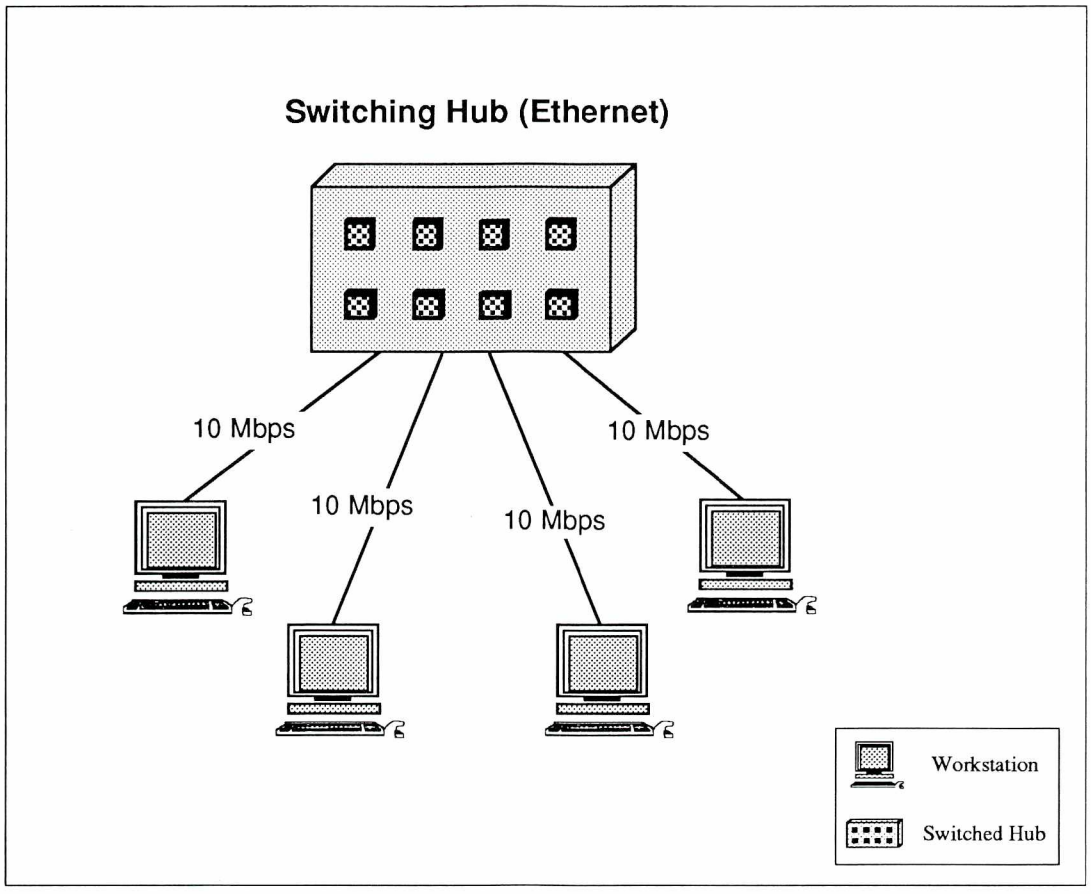

Figure 4: Diagram of high speed network interface

Internetwork Management

Ideally, internetwork management consists of central access to all information traveling across a distributed network including devices, segment statistics, and configurations. Effective internetwork management demands knowledge of network traffic patterns. Network segmentation should facilitate, rather than degrade, access to resources. To appropriately link communications, traffic patterns and loads should be considered in relation to required throughput, system capacity and LAN topologies. Filtering can restrict traffic to specific areas and limit unnecessary traffic from propagating to the network at large.

The type and quantity of network traffic directly impacts the productivity of end users. Internetwork management is essential to maintaining end-user productivity in a cost-effective computing environment. Access to network services and response time play important roles in supporting end-user productivity on enterprise networks. Network components such as servers, routers, bridges, hubs, switches, cabling, and software (network operating systems and user applications) also need to be managed across multiple internetwork links.

The goal of internetwork management is to ensure the connections between LAN segments operate smoothly and cost-effectively without impacting end users. In a distributed environment, data often travels across a connection from a service on one LAN segment to a service on another LAN segment, possibly via a WAN. Internetwork management supports this distributed architecture so the data appears as if it resides on a local connection.

In order to achieve this transparent connectivity across internetworks, two critical data translations are necessary. First, data must be translated from one physical media to another. This may involve a change to any or all of the following: physical interface to the network segment, network type, and available bandwidth.

Second, when a data packet passes across a network interface, the packet often requires translation from one communications protocol to another. This occurs for one or all of the following reasons: First, an encapsulating protocol may be used to facilitate addressing over the WAN. Second, encapsulation can enable bridges or routers to communicate more quickly. Third, a different frame format may be needed for transmission from token ring to Ethernet or vice versa. Finally, an encapsulating protocol can enhance the error control and correction capabilities of a wide area link. The communication protocol can be translated either from LAN to LAN, or from LAN to WAN.

For example, if a packet passes between two remote routers over a point-to-point WAN link, the packet is stripped of its LAN header and trailer information prior to the WAN transmission. The packet must require encapsulation in a router proprietary protocol for the WAN transmission. Finally, the packet goes through a repackaging upon reaching the destination LAN.

Five areas of management can improve smooth data translations between internetwork connections. These issues require attention to maintain optimum versatility and speed across internetworks:

- Bandwidth management
- Protocol management
- Bridge and router management
- Error management
- Configuration management

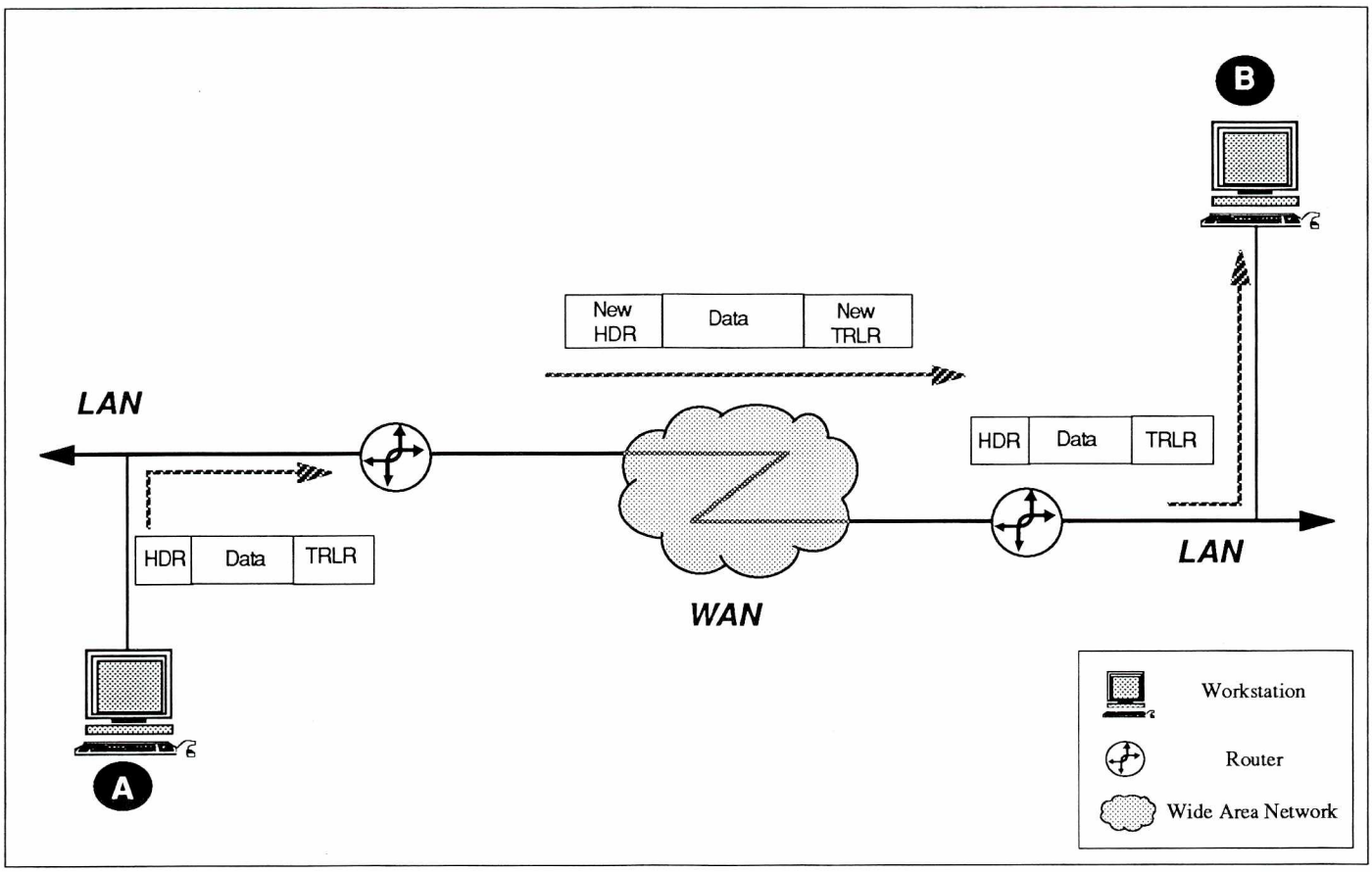

Figure 5: Frame encapsulation occurs when a packet travels between routers on either side of a WAN link

Bandwidth Management

To create a transparent connection for applications traveling across LAN and WAN links, bandwidth management is essential. Applications that operate over a distributed network and utilize wide area links require sufficient, but not excessive, bandwidth to send packets to the intended destination. If available bandwidth on either the LAN or the WAN connection is inadequate, the application may fail, adversely impacting employee productivity. If available bandwidth outpaces demand, the costs of distributed networks can unnecessarily skyrocket.

For example, if bandwidth shrinks from an Ethernet segment standard of 10 Mbps to a WAN connection of 56 Kbps, the internetwork devices have to perform significant data buffering to avoid data loss. Even with sufficient buffering, response time may suffer. To avoid this problem, sufficient bandwidth is required to accommodate bandwidth-intensive applications such as large file transfers or multimedia programs.

Conversely, access to virtually unlimited bandwidth across a WAN (e.g., a 45 Mbps DS3 connection) can be both costly and wasteful. High-speed WAN connections typically involve leasing or purchasing expensive equipment and facilities from third parties. Effective bandwidth management requires a balance between end-user application requirements and leased-line costs.

Initially, installation of low-speed, wide area connections between any two dispersed points on a network may be adequate. As new applications and more users are added to the distributed network, additional bandwidth may be needed. Installing a full mesh, point-to-point wide area topology where every wide area site is connected to every other site via a dedicated circuit can upgrade bandwidth availability. Alternatively, full mesh connectivity can be emulated through multiple virtual connections across a Wide Area Network. At that point, issues such as future network expansion, WAN interface availability, and network cost vs. direct network control need to be considered.

640 KByte Application Load Assuming 100 Percent Efficiency	
9.6 Kbps	9.1 minutes
38.4 Kbps	2.3 minutes
56.0 Kbps	1.6 minutes
112.0 Kbps	47.0 seconds
1.5 Mbps (T1)	3.5 seconds
6.4 Mbps (T2)	0.8 seconds
10.4 Mbps	0.5 seconds

Figure 6: Cost-effective bandwidth utilization requires appropriate link speeds to ensure adequate response times for end-user applications (Source: Telecommunications, July 1990)

Protocol Management

Effective protocol management also affects the performance of distributed internetwork links. With LAN-to-LAN internetworks, LAN segments operate using a common media access control layer while theoretically supporting a limitless number of upper-layer protocols. Traffic on a local LAN has full use of the local segment bandwidth. Because the LAN uses native protocols throughout its transmission, verifying the connection and data integrity is straightforward.

However, with LAN-to-WAN internetworks, some LAN protocols (especially those used in client/server applications) are far from "WAN efficient." For example, NetBIOS takes up a large amount of bandwidth when traveling from LANs to WANs because NetBIOS requires frequent acknowledgments and is prone to broadcasts over the WAN. When passing traffic across internetworks, the protocols carrying application data should incorporate maximum connection verification and error checking while adding minimum overhead to the application data. Unlike traffic on a local LAN segment, internetworks may create noticeable performance and cost penalties for traffic that must be repeatedly retransmitted or verified at the applications layer.

Effective protocol management balances data integrity against data throughput. Both applications and the protocols they support must be carefully managed to avoid potential problems. Protocol management addresses the following problems:

- **Unnecessary Broadcast Packets**

  Service advertisements and other broadcast packets may be appropriate to a local segment. In some instances, these packets do not need to traverse beyond the local LAN. When unnecessary packets broadcast across the distributed enterprise network, the excess traffic can affect internetwork links and end-user response times.

- **Redundant Connection Verification**

  Redundant connection occurs when a packet is encapsulated within a protocol that duplicates a control mechanism already existing in the original packet. For example, a packet containing a connection-oriented protocol such as LLC-type 2 could be encapsulated within another connection-oriented protocol such as HDLC for transmission across a wide area link.

- **Session or Connection Time-Outs**

  When a protocol or application designed for operation over a LAN is used in a distributed internetwork environment, session or connection time-outs can cause response time to degrade. Connection time-outs originate when a connection between two nodes cannot be maintained through the physical media. To minimize time-outs, locate devices closer to the resources the devices will use, or upgrade the processing capabilities of the device(s). Alternatively, migrate to a protocol, such as TCP/IP, that will automatically reconfigure its acknowledgment time in response to an extended round-trip delay.

Bridge and Router Management

Routing problems become apparent when traffic does not move along anticipated network paths. In a distributed client/server network this poses a geographic challenge as well as a technical one. As bridges and routers are further distributed, the network control becomes more challenging.

Although the core data associated with an application remains unaffected during transmission across one or more network interfaces, that same data 'package' may be sent in several different protocol 'envelopes' during that period. To ensure data integrity across the internetwork, the transition from one enveloping protocol to another must be seamless.

The bridge or router at the network interface must be capable of bit stripping, framing, addressing, and segmenting data packages in a flawless and timely fashion. In addition, the bridge or router must operate as a separate protocol engine for each segment of the internetwork. This provides protocol functions such as connection acknowledgments, timing, and error checking. When a problem occurs, internetwork management tools should pinpoint the location and severity of the problem.

The following bridge and router issues can affect overall internetwork performance:

- **Clean Protocol Encapsulation**
  For end devices on either side of the internetwork connection to operate efficiently (or at all), the communicating nodes must be set up to encapsulate LAN packets in the same WAN protocol envelope. In addition, elements such as response times and window size should also be matched between devices.
- **Correct Address Translation, Configuration, and Forwarding**
  In order for internetworking to be successful, addressing must be configured properly for each topology frames transverse. For example, due to the different manners in which MAC addresses are received, a token ring-to-Ethernet bridge should correctly bit-reverse the MAC addresses of frames passing from one topology to the other and correctly interpret either address. Bridges or routers (and all other devices) operating on an IP network require correct configurations with respect to subnetworks to avoid duplicate addresses. Finally, bridges or routers should correctly map addresses on the LAN-side interface to the appropriate WAN side-address or end-point. For example, routers should provide a correlation between a frame relay Data Link Connection Identifier (DLCI) and an IP address.
- **Correct Protocol Interpretation and Response**
  Just as communicating devices on the LAN must interpret and respond to a common protocol, this is equally important across the internetwork. To facilitate data transmission and network maintenance, both devices on either side of an internetwork link must be running compatible versions of a protocol stack. Consistency between two remote devices should include both frame format and upper-layer protocols. For example, if two routers are communicating over an X.25 WAN, both devices must understand each other's Data Network Identification Code (DNIC) addresses to send and receive data. Compatible frame formats, or data link protocols such as Link Access Procedure Balance (LABP), are also required for correct interpretation and response across an internetwork link.
- **Fast Processing at the Device Interface**
  Intensive frame processing may cause data loss by dropping frames. Similarly, intensive processing may significantly delay frame transmission times. To avoid data loss, make sure the bridge or router buffer has enough memory available to buffer any incoming frames. Minimize time delays using a dedicated bridge or router with a fast processor, such as a 80486 or above. This guarantees the processor spends 100% of its time processing frames without being burdened by overhead tasks.

Error Management

Successful internetwork performance can be measured by the efficiency of an application. The application's execution should not affect end-user response time, regardless of whether the application occurs locally or in an internetworked environment. Application delays can result from internetwork device errors and/or media errors. These delays manifest themselves to the end user in various ways such as slow application performance, complete application lock-up, or network crash. Internetwork management should address the following types of errors:

- Device hardware errors include poor physical interface connections or a bad network interface card.
- Device software problems include translational errors resulting in incorrectly addressed packets or packets that contain bit errors.
- Encapsulation protocol errors occur when two internetworking devices are unable to communicate because they implement different versions of the same protocol.
- Media errors can occur when a wide area link introduces multiple physical errors into the bit stream. The number of physical errors influences whether the wide area data link protocol should be connection-oriented (e.g., X.25), or connectionless (e.g., frame relay, or point-to-point Protocol).

In addition, errors related to bandwidth, protocol, and bridge and router management can all contribute to communication delays on an internetwork. In distributed network environments with multiple network devices and segments, the process of error management is essential to pinpoint the cause of internetwork delays.

Configuration Management

Because of the constantly changing and geographically dispersed nature of enterprise networks, configuration management can be the most challenging aspect of internetwork management. Configuration management entails maintaining an accurate picture of the network's devices, users, addresses, and topologies. Configuration management helps you plan, manage, and troubleshoot the performance of internetworks with new users, additional devices, and distributed segments.

To facilitate bandwidth management, configuration management requires a current picture that reflects new segments added to the network. Without the ability to map new configurations, additional traffic could cause congestion problems. Configuration management also facilitates the security process in enterprise environments. For example, your network monitoring device should continuously update user lists to validate documented and undocumented users.

Finally, configuration management supports the first step in the troubleshooting process. Network maps help correlate a NIC address with an end user's physical location to verify the physical layer, or hardware.

Keeping a current map of the network sets the stage for security, device reconfiguration, troubleshooting, and future network expansion in enterprise environments.

Conclusion

As enterprise networks expand, the process of delivering data from one LAN segment to another becomes increasingly complex. From dial-up modems to sophisticated ATM switches, internetworks lay the infrastructure for traffic to move efficiently between nodes, between LANs, and between LANs and WANs. Effective internetwork management supports the geographical reach of your distributed network.

Bandwidth management helps ensure sufficient, but not excessive, bandwidth availablility to support end-user productivity and minimize leased-line costs. Protocol management balances data integrity against data throughput. Bridge and router management helps ensure traffic moves along anticipated nework paths. In distributed network environments with multiple network devices and segments, the process of error management is essential to pinpoint the cause of internetwork delays. Finally, configuration mnagement helps you keep up to date on the changing nature of devices and applications on distributed internetworks.

The accompanying paper outlines how to use Network General's products in the process of internetwork management to plan, troubleshoot, maintain, and expand your enterprise network for maximum efficiency.

Please contact your Network General sales representative or call 1-800-Sniffer (1-800-764-3337) for further information on how to plan, implement, and manage your distributed internetworks.

Thank you for your interest in Network General.

Corporate Headquarters

Network General Corporation
4200 Bohannon Drive
Menlo Park, CA 94025 USA
TEL: (415) 473-2000
FAX: (415) 321-0855

U.S. Sales Offices
Menlo Park, CA (800) 846-6601

Eastern Region
Wakefield, MA (617) 224-1244
Red Bank, NJ (908) 758-0062
Rockville Center, NY (516) 766-4100
Westlake, OH (216) 892-1330
Dunn Loring, VA (703) 641-0074

Central Region
Atlanta, GA (404) 491-3800
Oakbrook Terrace, IL (708) 574-5770
Carrollton, TX (214) 386-6384

Western Region
Phoenix, AZ (602) 598-0335
Anaheim, CA (714) 939-9188
Santa Clara, CA (408) 982-1910
Westlake Village, CA (818) 597-9012

Asia
Network General Asia
111 Northbridge Road #11-04
Peninsula Plaza, Singapore
TEL: (65) 336-0431
FAX: (65) 339-5291

Australia
Network General Australia PTY Ltd.
Level 20, 99 Walker Street
North Sydney, NSW, 2060 Australia
TEL: (61) 2-911-7770
FAX: (61) 2-911-7750

Europe

Belgium
Network General Europe N.V.
Belgicastraat 4
B-1930 Zaventem, Belgium
TEL: (32) 2-725-6030
FAX: (32) 2-725-6639

France
Network General France S.A.R.L.
Atria, 21 Avenue Edouard Belin
F-92566 Rueil Malmaison
Cedex, France
TEL: (33) 1-47-16-9900
FAX: (33) 1-47-16-9907

Germany
Network General GmbH
Mettmanner Strasse 24
D-40233 Duesseldorf, Germany
TEL: (49) 211-98-4050
FAX: (49) 211-730-8839

Switzerland
Network General NGC AG
Lerzenstrasse 21
CH-8953 Dietikon Switzerland
TEL: (41) 1-742-2550
FAX: (41) 1-742-2554

North America

Canada
Network General Canada, Ltd.
9225 Leslie Street, Unit 7
Richmond Hill, Ontario L4B 3H6
Canada
TEL: (905) 882-7905
FAX: (905) 882-9454

South America

Brazil
Network General do Brasil
Avenida Paulista, 1439, Cj. 52
01311-200 - Sao Paulo - S.P., Brazil
TEL: (55) 11-289-7666
FAX: (55) 11-289-6215

Latin America
Network General Latin America & Caribbean
3609 Cleveland Street
Hollywood, FL 33021
TEL: (305) 981-3388
FAX: (305) 981-9470

Network General products are available from sales offices and distributors worldwide.

GSA Schedule Number—GSOOK92AGS61Ø9 PSØ8

Printed on recycled paper. P/N 24153-001 10/94

Forward product suggestions to Network General via the Internet to: *suggestions@ngc.com*